



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/075,926	02/14/2002	David Willming	01-873	1692

7590 02/23/2006

McDonnell Boehnen Hulbert & Berghoff
32nd Floor
300 S. Wacker Drive
Chicago, IL 60606

EXAMINER

CHAI, LONGBIT

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 02/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/075,926	Applicant(s) WILLMING ET AL.	
	Examiner Longbit Chai	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 January 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Original application contained claims 1 – 25. Claims 1, 5, 6, 9, 11, 13, 14 and 20 – 24 have been amended; and new claims 28 and 29 have been added in an amendment filed on 01/13/2006. The amendment filed have been entered and made of record. Presently, pending claims are 1 – 25.

Response to Arguments

2. Applicant's arguments with respect to instant claims have been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, 2, 8 – 13, 15, 19, 21, 23 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind (Patent Number: 6823454), in view of Rowney (Patent Number: 5996076).

As per claim 1 and 21, Hind teaches a method for automatic installation of a digital certificate on a cable modem in a data-over-cable system, the method comprising:

determining whether a digital certificate is installed on the cable modem (Hind: Column 14 Line 1 – 3, Column 9 Line 28 – 31 and Column 8 Line 14 – 16: the wireline connections using the physical cable media must incorporate a cable modem within a server system, namely, CMTS (Cable modem Termination System), which is well known in the field); if not, generating a digital certificate filename on the cable modem (Hind: Column 13 Line 58 – 64). Hind teaches, if not, downloading the device certificate from the server device to client device (Hind: Column 13 Line 58 – 64); however, Hind does not disclose generating a digital certificate filename on the cable modem for downloading purpose.

Rowney teaches generating a digital certificate filename on the cable modem (Rowney: Column 4 Line 54 – 63 and Column 163 Line 22 – 26).

sending a digital certificate request including the digital certificate filename to a predetermined network server; receiving a digital certificate file including at least one digital certificate from the network server; and storing the at least one digital certificate received from the network server on the cable modem (Rowney: Column 4 Line 54 – 63, Column 154 Line 62 – 65 and Column 163 Line 22 – 24); and

wherein the digital certificate is required to authenticate the cable modem on a Cable modem Termination System (CMTS) (Hind: Column 9 Line 28 – 31, Column 8 Line 14 – 16 & Column 3 Line 54 – 56 and Column 13 Line 13 – 17).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rowney within the system of Hind because (a) Hind teaches a dynamic / flexible mechanism to obtain a device certificate during initialization of the device (Hind: Column 13 Line 58 – 60) and (b) Rowney teaches a more secure and flexible certificate delivery and installation method over a public communication system, such as internet (Rowney: Column 154 Line 62 – 65, Column 163 Line 22 – 24 and Column 4 Line 1 – 4).

As per claim 2 and 15, Hind as modified teaches having stored therein instructions for causing a processor to execute the method of claim 1 (Hind: Figure 1A).

As per claim 8, Hind as modified teaches obtaining a globally routable network address on the cable modem prior to sending the digital certificate request to the network server (Hind: Column 13 Line 29 – 40: the Domain Name Server DNS/DHCP system assures that both the server and client (i.e. server device and client device) must use a globally routable network address (i.e. global IP address) in order to access the network entities on external networks); and employing the globally routable network address for sending the digital certificate request to the network server (Hind: Column 13 Line 29 – 40: the request / response are exchanges with standard global IP protocol messages).

As per claim 9, Hind as modified teaches retrieving network address information from at least one data packet sent from at least one customer entity (Hind: Column 2 Line 63: masquerading attack as disclosed by Hind is a way to retrieve network address information from at least one data packet sent from at least one customer entity); and obtaining a physical address of a network gateway associated with the at least one customer entity (Hind: Column 2 Line 21 – 48: the MAC address (besides the IP address) of the router / gateway is needed for the routing protocol before the messages can be successfully routed over the networks via network router located on its own network segment (or subnet)).

As per claim 10, Hind as modified teaches the network address information comprises on Internet Protocol address and a Medium Access Control address associated with the customer entity (Hind: Column 2 Line 16 – 67: both Internet Protocol address and a Medium Access Control address are required for standard IP network protocol).

As per claim 11, Hind as modified teaches validating the at least one digital certificate received from the network server prior to storing the at least one digital certificate on the cable modem (Hind: Column 14 Line 12 – 14).

As per claim 12, Hind as modified teaches the at least one digital certificate comprises a device digital certificate (Hind: Column 13 Line 13 – 14).

As per claim 13, Hind as modified teaches the at least one digital certificate further comprises a cable modem manufacturer digital certificate (Hind: Column 14 Line 2).

As per claim 19, Hind as modified teaches the at least one digital certificate for the cable modem is generated on the network server (Hind: Column 13 Line 58 – 64).

As per claim 23, Hind as modified teaches wherein the network server's address is installed on the cable modem prior to requesting, the digital certificate from the predetermined network server (Hind: Column 1 Line 40 – 42: constant IP address).

As per claim 24, Hind as modified teaches the cable modem is further arranged to install the digital certificate in a memory unit upon receiving the digital certificate from the network server (Hind: Column 13 Line 58 – 64).

4. Claims 3 – 7, 16, 18, 22 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind (Patent Number: 6823454), in view of Rowney (Patent Number: 5996076), in view of Loukianov (Patent Number: 6715075).

As per claim 3, 18 and 22, Hind as modified does not disclose the network server comprises a Trivial File Transfer Protocol server.

Loukianov teaches the network server comprises a Trivial File Transfer Protocol server (Loukianov: Column 1 Line 65 – 67, Column 2 Line 11 – 22 and Column 3 Line 45 – 55).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Loukianov within the system of Hind as modified because (a) Hind teaches device certificate authentication mechanism and (b) Loukianov teaches providing a secure device certificate method for cable modem systems by using a hash signature (Loukianov: 2 Line 11 – 22).

As per claim 4 and 25, Hind as modified teaches the digital certificate comprises an X.509 security digital certificate (Loukianov: Column 3 Line 54 – 55). Same rationale of combination applies here as above in rejecting the claim 3.

As per claim 5 and 16, Hind teaches a device ID is included in the device certificate (Hind: Column 3 Line 60 – 61). However, Hind does not disclose expressly a digital certificate filename comprises using a type of the cable modem, a physical address of the cable modem and an authentication data string.

Loukianov teaches a digital certificate filename comprises using a type of the cable modem, a physical address of the cable modem and an authentication data string (Loukianov: Column 2 Line 50 – 54 and Column 2 Line 19 – 20; Hind: Column 3 Line 60 – 61: Examiner notes a certificate filename is used to uniquely identify a device certificate and thereby certificate ID is equivalent to a certificate filename. Device

certificate ID includes a device ID (Hind: Column 3 Line 60 – 61) and, besides, the cable modem device can also uniquely identified by MAC address and a certificate can be uniquely identified by certificate hash value as taught by Loukianov (Loukianov: Column 2 Line 50 – 54 and Column 2 Line 19 – 20). Therefore, a digital certificate filename comprises using a type of the cable modem, a physical address of the cable modem and an authentication data string).

Same rationale of combination applies here as above in rejecting the claim 3.

As per claim 6, Hind as modified teaches the authentication data string is generated on the cable modem by applying a hash function to at least one configuration setting associated with the cable modem (Loukianov: Column 2 Line 19 – 20).

As per claim 7, Hind as modified teaches the at least one configuration setting comprises a MAC address, a serial number or a secret string (Loukianov: Column 2 Line 19 – 20).

5. Claims 14 and 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hind (Patent Number: 6823454), in view of Rowney (Patent Number: 5996076), and in view of Kent (Patent Number: 6671804).

As per claim 14, Hind teaches a method for providing digital certificates to at least one network device in a data-over-cable system (Hind: Column 9 Line 28 – 31 and

Art Unit: 2131

Column 8 Line 14 – 16: the wireline connections using the physical cable media must incorporate a cable modem within a server system, namely, CMTS (Cable modem Termination System), the method comprising:

the digital certificate is required to authenticate the cable modem on a Cable modem Termination System (CMTS) (Hind: Column 3 Line 54 – 56 and Column 13 Line 13 – 17).

Hind does not disclose expressly receiving a digital certificate request including a digital certificate filename on a network server from a network device.

Rowney teaches receiving a digital certificate request including a digital certificate filename on a network server from a network device (Rowney: Column 4 Line 54 – 63 and Column 163 Line 22 – 26);

generating at least one digital certificate for the network device; and providing the at least one digital certificate from the network server to the network device (Rowney: Column 4 Line 54 – 63 , Column 154 Line 62 – 65 and Column 163 Line 22 – 24).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rowney within the system of Hind because (a) Hind teaches a dynamic / flexible mechanism to obtain a device certificate during initialization of the device (Hind: Column 13 Line 58 – 60) and (b) Rowney teaches a more secure and flexible certificate delivery and installation method over a public communication system, such as internet (Rowney: Column 154 Line 62 – 65, Column 163 Line 22 – 24 and Column 4 Line 1 – 4).

Hind as modified does not disclose expressly authenticating the request on the network server using at least one parameter specified in the digital certificate filename.

Kent teaches authenticating the request on the network server using at least one parameter specified in the digital certificate filename (Kent: Column 10 Line 9 – 22).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kent within the system of Hind as modified because (a) Hind teaches device certificate authentication mechanism and (b) Kent teaches providing a enhanced secure validation mechanisms by verifying the certificate requests information from a plurality of requesters (Kent: Column 2 Line 59 – 63, Column 10 Line 9 – 40).

As per claim 20, Hind as modified does not disclose expressly requesting a digital certificate from a second network server upon receiving the digital certificate request from the cable modem; and receiving the digital certificate on the network server from the second network server, wherein the second network server comprises a certificate authority server.

Kent teaches requesting a digital certificate from a second network server upon receiving the digital certificate request from the cable modem; and receiving the digital certificate on the network server from the second network server, wherein the second network server comprises a certificate authority server (Kent: Figure 1 Element 110/120/130 and Column 4 Line 27 – 30).

Same rationale of combination applies herein as above in rejecting the claim 14.

6. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hind (Patent Number: 6823454), in view of Rowney (Patent Number: 5996076), in view of Loukianov (Patent Number: 6715075), and in view of Kent (Patent Number: 6671804).

As per claim 17, Hind as modified does not disclose generating an authentication data string on the network server; and comparing the authentication string generated on the network server with the authentication data string specified in the received digital certificate filename.

Kent teaches generating an authentication data string on the network server; and comparing the authentication string generated on the network server with the authentication data string specified in the received digital certificate filename (Kent: Column 10 Line 9 – 40: the authentication string is the public key of the requester).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kent within the system of Hind as modified because (a) Hind teaches device certificate authentication mechanism and (b) Kent teaches providing a enhanced secure validation mechanisms by verifying the certificate requests information from a plurality of requesters (Kent: Column 2 Line 59 – 63, Column 10 Line 9 – 40).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100